The following is a sequence of questions and answers regarding the Arizona Network (*AZNet*) telecommunications program….Security. If you have any questions, please submit them via the *AZNet* website: www.aznet.gov or call the Telecommunications Program Office (TPO) at 602-364-1106.

Security

1. How is the firewall rule base policy between an agency and *AZNet* coordinated?
Response: The state IP Address and Security Committee has developed a minimum firewall policy that is compliant with GITA standards. Exceptions to this policy are presented to the committee for approval. Agency firewalls managed by *AZNet* will be held to that minimum policy. *Agenda items and exceptions should be sent to Dan Oseran (Daniel.Oseran@Calence.com).*

2. How are firewall rule base changes reviewed and approved?
Response: Agencies will document their rules and request firewall rule changes as needed via the MAC process. An agency manager must provide approval. These firewall changes will be reviewed by the *AZNet* Security Engineering team in conjunction with the requesting agency. If an Agency has a dedicated security team, that team will be contacted to ensure the change is in accordance with agency policies, GITA standards and the IP Address and Security Committee minimums. Agencies are encouraged to create basic connectivity test plans to validate that new rules are functional and existing rule policies are not impacted. The agencies must be involved with the rule base requirements gathering and the post-implementation testing to confirm that all connectivity remains in effect. Changes to the firewalls themselves are generally limited to after normal business hours to reduce the risk of impacting secondary systems during peak use times.

3. How are alerts reported to the agencies and how will they be resolved? How are agency custom attack signatures communicated to and maintained by *AZNet*?
Response: If traffic in the network causes extreme performance degradation or is deemed a high security threat to an agency, *AZNet* can take immediate reactive measures to block the malicious traffic. If the traffic block is put into operation by blocking the Internet source, *AZNet* must communicate this block

to the agency security contacts as soon as possible (within 2 hours). If the traffic block is put into operation by blocking an agency source, *AZNet* must immediately communicate this block to the source agency contacts.

If traffic entering the network causes no performance degradation and is deemed a medium or low security risk (i.e. the traffic is reminiscent of a malicious attack), the agency to which the traffic is directed shall be contacted by *AZNet* as soon as practicable. The agency will have 8 hours from time of *AZNet* notification to rectify the issue. If, the agency is unable to rectify the issue within this time, *AZNet* may, at its discretion and for the benefit of the majority of the state agencies, block the traffic.

4. Does *AZNet*'s IPS only snipe sessions where packets match a signature and are determined to be bad? Or, does it actually ban IP addresses, networks, etc? How does *AZNet* mitigate the potential for DoS attacks leveraging this type of active response behavior?
Response: IPS policies will be developed as part of the detailed Security Plan development and implementation process. Generally speaking, only sessions (or individual packets in a session instance) positively identified as malicious are restricted. This constraint is implemented to prevent an active blocking response resulting in a denial of service to legitimate hosts (e.g., session spoofing). Additional controls, including IDS, will be combined with IPS services to ensure identification and appropriate response (active or manual) without negative impact to business services.